FUTURE GOVERNMENT INSTITUTE
Powered by Public Sector Network

CYBERSECURITY AS A PUBLIC GOOD: SOVEREIGNTY, OPEN SOURCE, AND THE NEW CYBER IMPERATIVE

EXECUTIVE SUMMARY | VOL.28 | WESTERN AUSTRALIA

Curtin University

IN BRIEF

This PSN research roundtable convened public sector technologists, cybersecurity strategists, local government digital leads, university academics, and open-source industry representatives to examine the evolving conditions required for a cyber-resilient Australia. The conversation moved beyond surface-level calls for public-private collaboration and instead uncovered structural and philosophical challenges inhibiting progress.

Participants examined how legacy systems, fragmented procurement models, and short political cycles undermine strategic continuity, and proposed new roles for universities as solution co-designers, product validators, and knowledge-transfer brokers. The discussion highlighted growing appetite among digital leads to adopt open-source solutions and cultivate in-house engineering capabilities but acknowledged widespread institutional hesitation around risk, trust, and procurement rigidity.

Significant attention was paid to how long-term partnerships, rather than transactional funding relationships, are vital to sustaining innovation across government, industry, and academia. Calls for cross-sectoral innovation budgets, curated talent pipelines, and practical trials for open-source security were common. Above all, participants argued that digital resilience cannot rely on vendor guarantees alone: government must be a competent custodian of its systems.

By **Patrick Joy** | Head of Research & Analysis | **Public Sector Network**

KEY THEMES AND INSIGHTS

FOUNDATIONS BEFORE FIREWORKS: IS CYBERSECURITY BORING?

While the public narrative around cybersecurity often spotlights high-profile threats, participants repeatedly stressed that the most urgent work involves tackling mundane but mission-critical technical debt. For example, one health leader noted their organisation was still operating on “1978 Wi-Fi” while simultaneously rolling out a full digital patient record ecosystem, creating a vastly expanded threat surface with fragile defences.

This contradiction between public investments in "the next digital widget" and the neglect of basic digital hygiene echoed across agencies. The consensus was clear: resilience begins with disciplined, well-funded infrastructure and asset management, not just innovation theatre.

ACADEMIA AS HONEST BROKER: BUILDING TRUST BETWEEN TECH AND PROCUREMENT

Universities were repeatedly positioned as a trusted third party to help navigate the increasing complexity of cybersecurity product landscapes. Several leaders expressed frustration at the opacity of vendor claims and the absence of neutral validators. One compelling proposal was for universities to act as non-commercial evaluators of competing solutions, providing diagnostic support and publishing independent implementation reviews.

This role would allow agencies to make informed decisions free from vendor lock-in, while giving universities a structured mandate to contribute strategically outside of student placement programs.

DESIGNING FOR RESILIENCE, NOT JUST COMPLIANCE

Policy frameworks and risk registers can support governance, but participants noted they do little to develop the adaptive capability required for cyber resilience. Speed, responsiveness, and system-level awareness were all cited as lacking in many government environments.

Participants advocated for a strategic shift: instead of treating cybersecurity as an isolated compliance domain, it should be embedded into product design, procurement, and workforce planning. Governments must move beyond “building for auditors” and instead design systems that degrade gracefully under stress.

THE SOVEREIGNTY PLAY: OPEN SOURCE AS STRATEGIC INFRASTRUCTURE

Open-source platforms were discussed as a critical (yet underutilised) pathway to building digital sovereignty. Several contributors highlighted that while Australia has significant capacity to consume open-source software, it lacks the systemic enablers to shape, govern, or extend these platforms independently.

Universities and open-source firms were seen as ideal partners for growing sovereign capability. However, speakers also warned that success requires more than code access. Training, support ecosystems, and lifecycle funding are essential to operationalise open-source solutions at scale within the public sector.

CHALLENGES AND BARRIERS

PROCUREMENT PARALYSIS AND POLICY CATCH-22S

A dominant barrier raised was the rigidity of procurement systems. While innovation may emerge from agile partnerships or hackathons, translating these ideas into funded solutions typically requires open tenders and formal risk assessments. This creates a contradiction: governments want experimentation, but only if it follows fixed pathways.

Several participants lamented the impossibility of receiving public funding without an existing use case or first customer—yet public sector organisations are unable to become that first customer without going to tender. This self-reinforcing loop was seen as a major inhibitor to scaling novel technologies.

INCENTIVES MISALIGNED WITH SYSTEMIC OUTCOMES

Short-termism emerged as a cross-cutting issue. Election cycles, budget reporting windows, and narrow funding lines were seen as poorly suited to the long timelines required to develop sovereign capabilities or migrate from legacy systems.

Even innovation funding often reinforces this bias. One participant described how pilots are funded as one-off proofs-of-concept without any sustainable path to scale or maintain the result.

FUTURE FOCUS AREAS

ESTABLISHING INNOVATION ALLOCATION WITHIN OPERATIONAL BUDGETS

Participants proposed earmarking dedicated innovation funds within existing operational portfolios to explore early-stage ideas without triggering complex procurement pathways. This would allow agencies to co-develop, trial, and iterate on experimental solutions—including partnerships with universities—before formalising broader procurement.

MATURING OPEN SOURCE PROCUREMENT PATHWAYS

Open source solutions are often dismissed due to perceptions of instability, unclear vendor support, or lifecycle risk. A future focus should be on developing rigorous validation pipelines for open source technologies, including university-led testbeds that simulate implementation environments and generate evidence for security, scalability, and sustainability.

STRATEGIC WORKFORCE PROGRAMS ACROSS GOVERNMENT AND ACADEMIA

Rather than isolated internships, participants supported systemic programs that embed university talent within agencies for sustained capability building. This includes pathways for researchers to co-develop policy and product architectures and return to academia with practical insights.

Developing a federated graduate program across government, designed in tandem with universities, could also help address ongoing workforce shortages in cybersecurity and adjacent digital skills.

INNOVATIVE IDEAS AND CASE STUDIES

1. UNIVERSITIES AS CO-DESIGNERS OF SOVEREIGN INFRASTRUCTURE

A recurring concept was repositioning universities as infrastructure architects. Rather than commissioning discrete projects, governments could partner with research institutions to shape foundational service layers—from open-source EMRs in health, to interoperable data platforms in transport.

Such arrangements would not only create bespoke systems better aligned to local policy needs, but also reduce dependence on multinational vendors and support the growth of national IP.

2. OPEN SOURCE TESTBEDS FOR INFORMED DECISION-MAKING

In one case example, a research institution helped a UK government department assess competing cybersecurity solutions by developing side-by-side testbeds for open-source and proprietary systems. This enabled non-partisan comparison of costs, features, and security implications before procurement.

Participants called for similar test environments to be established in Australia, potentially through state-supported labs hosted within universities and operated in partnership with digital government agencies.

3. WHOLE-OF-GOVERNMENT CYBERSECURITY WORKING GROUPS

Western Australia's security working group was praised for enabling collaboration across departments. This informal but consistent structure has fostered improved situational awareness and shared practices, and helped lift sector-wide capabilities without requiring structural reform. Participants suggested that this working model could be deepened through academic involvement—not just to observe, but to support co-design of strategic roadmaps, solution scoping, and data-informed policy shifts.

STRATEGIC OUTCOMES AND RECOMMENDATIONS

IMMEDIATE ACTIONS

- **Establish cross-agency innovation funds** to enable experimentation with academic partners outside standard procurement.
- **Launch open-source capability reviews** led by universities to identify opportunities for sovereign infrastructure.
- **Formalise whole-of-government cyber** working groups with rotating university advisory roles.

MEDIUM-TERM GOALS

- **Develop open-source testbed facilities** within universities, allowing departments to trial systems pre-procurement.
- **Co-design graduate development programs** between agencies and universities with structured post-placement feedback loops.
- **Establish academic residencies** within government teams focused on strategic design and capability uplift.

LONG-TERM VISION

- **Position universities as trusted infrastructure partners**, not just research collaborators, with funding mechanisms aligned to co-design and validation functions.
- **Build sovereign open-source ecosystems**, anchored in Australian academic and public sector institutions.
- **Shift from transactional to relational procurement**, favouring long-term partnerships over short-term tenders to foster adaptive, resilient digital systems.

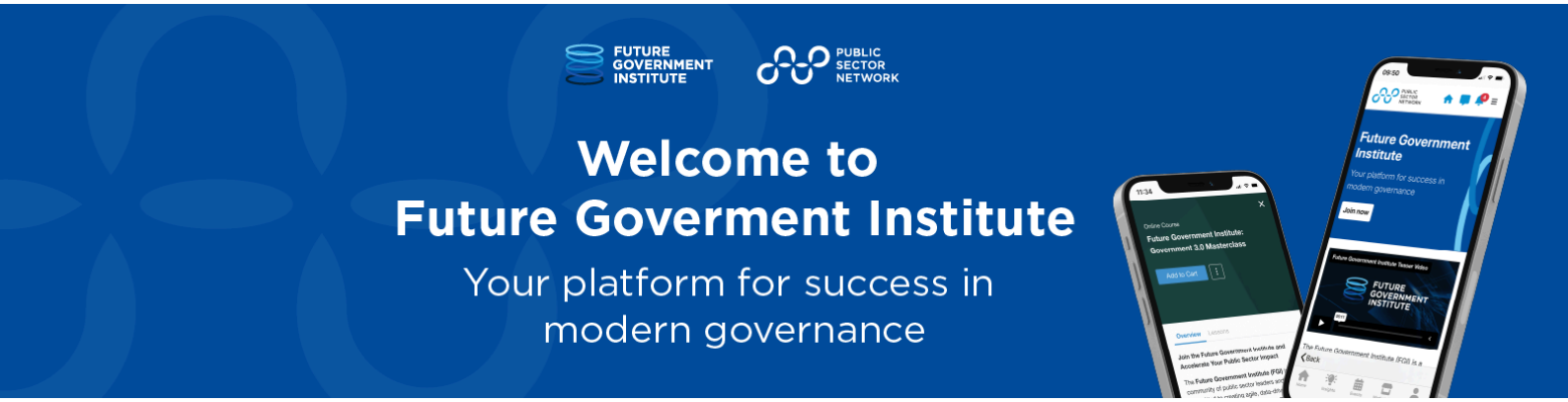
ABOUT THE FUTURE GOVERNMENT INSTITUTE (FGI) RESEARCH COUNCIL

We've been able to engineer a new program antithetical to the classical red tape, administration, and risk-aversion that impedes innovation.

Public Sector Network has recently launched The Future Government Institute (FGI), a global hub for forward-thinking public sector leaders, innovators, and practitioners dedicated to shaping the next era of governance.

Our mission is to empower government professionals with the tools, insights, and networks needed to drive meaningful transformation - https://publicsectornetwork.com/future-government-institute/

Leveraging our extensive connections, we are uniting the sharpest minds from government, academia, and industry via monthly research-driven roundtables, hosted at esteemed national centres of research, courtesy of university partners across Australia and New Zealand.



ABOUT PUBLIC SECTOR NETWORK

Public Sector Network is a research company that represents public sector professionals across Australia, Canada, New Zealand, and the USA. It develops roundtables, seminars, and conferences to suit current areas of interest to government agencies and their suppliers.

PSN's growing community spans across federal, state, and local government departments, healthcare, and education, allowing members to share information, access the latest in government innovation, and engage with other like-minded individuals on a secure and closed-door network.

AUSTRALIA / NEW ZEALAND
P +61 2 9057 9070
E INFO@PUBLICSECTORNETWORK.COM.AU

USA
P +1 (647) 969 4509
E HELLO@PUBLICSECTORNETWORK.COM

CANADA
P +1 (647) 459 8904
E CONTACT@PUBLICSECTORNETWORK.CO

Public Sector Network (Australia) Pty Ltd
ABN - 46 617 870 872 20-40
Meagher Street, Chippendale, Sydney NSW 2008, Australia